KOSKIE MINSKY

JUSTICE MATTERS

THE NEW CONCERNS OF WORKPLACE PRIVACY – TECHNOLOGY

By Nancy Shapiro, Partner and Jenna Bontorin, Student-at-Law

A. Overview

We live in the information age. Sometimes, we are seeking information we need, while other times, it is just information we "want". Just because the technology exists, many have the urge to get it! This means, as an employer, you will inevitably face the concerns of employee privacy. As technology evolves and as members of society become more concerned with their privacy generally, we see the rising need for the workplace to respond. It becomes apparent that, as employers introduce new technology for use in the workplace, it is necessary to implement policies that are appropriate and that the methods being employed are "reasonable".

From inherent differences in the power dynamic in a unionized vs. non-unionized environment, we often see challenges to infringements of employee privacy in the non-unionized context. The principles are applicable to workplaces in general though, and the cases below are a useful guide when considering the implementation of new technology in the workplace.

We will focus on technological advancement in four areas that create new concerns for workplace privacy: 1) devices in vehicles; 2) devices for entry control; 3) payment mechanisms; and, 4) pre-hiring screening.

There are a number of risks and issues that employers should consider while they continue to introduce new technologies into certain parts of their workplaces. While some of these updates are quite new and have not yet been considered by the courts or at arbitration, trends in past cases can demonstrate that the following should always be considered when implementing changes in the workplace that may affect employees' privacy rights:

- First, an employee should be informed of these systems when they accept the job (a straightforward example is if any privacy concerns are to be a condition of employment).
- Second, an employee should always be advised of technology updates in the workplace as they occur, and policies to deal with concerns should always be in place.
- Third, an individual's reasonable expectation of privacy is considered under the applicable statutes and at common law, so the least invasive method should always be considered.

As a general rule, whether or not privacy is protected by law or contract, striking the right balance with respect to privacy will lead to greater employee trust and acceptance to foster a better employer-employee relationship.

B. Devices in Cars

1. GPS Tracking

When programmed to do so, this technology can track the location of a vehicle and may record and/or report location of the vehicle. This technology can record/report speed, including speed relative to posted speed limits, and other driving related information such as movement, gas usage, distance and route travelled.

A recent Ontario Labour Relations Board decision[1] considered the introduction and use of such tracking devices in company vehicles. These devices provided information about aspects of the vehicle's use and location, and also monitored whether the vehicle was on or off, irrespective of time of day. The devices did not consider whether or not the driver was on duty or using the vehicle during "working hours".

The union asserted that the introduction of these devices was an unreasonable change in working conditions and an invasion of privacy of members. The company's position was that it is entitled to modernize its equipment and to introduce efficiencies in operation. One of the main disputes was whether employees who take vehicles home have ever been entitled to personal use of those vehicles. The union's evidence was that they had, and practices included use for such things as: grocery shopping, medical visits, attendance at union meetings, and stopping for dinner on the way home. The Board, however, ruled in favour of the employer and determined that the tracking device was a legitimate way to protect the employer's asset.

2. Photographing and Recording

The continuous development of more sophisticated and cheaper technology effectively permits companies to have constant connectivity to their equipment, allowing management to monitor the use and allocation of company assets in real-time and even relay a live video or take a recording of events inside or around a vehicle.

This issue was front and centre in *Brink's Canada Ltd. v. Childs*.[2] Brink's admitted to their practice of trucks being equipped with an advanced GPS tracking system and with additional internal and external video surveillance, which allow operators to see potential suspicious activity in a 360 degree arc around the vehicle. While privacy interests were not specifically at issue, the Occupational Health and Safety Tribunal did examine the merits of having such a system in place, saying those measures were developed with the purpose of enhancing the protection of employees while carrying out an activity that, by its very nature, inherently presents risks.

---

[1] *International Union of Elevator Constructors, Local 50 v. Otis Canada Inc.*, 2013 CanLII 3574 (ON LRB).
[2] *Brink's Canada Ltd. v. Childs*, 2017 CarswellNat 1972 (Canada Occupational Health and Safety Tribunal).

Short of security concerns, implementing surveillance of employees should be approached with caution. For example, in *Colwell v. Cornerstone Properties Inc.*, the employee had been working for two years when she discovered a camera had been installed in the ceiling of her office since she started employment. The court held the employment contract contained an implied term when the contract was entered into, that each party would treat the other in good faith and fairly, throughout the existence of the contract. The employer's implementation of surveillance without the employee's knowledge was a breach of this implied term and violated the employee's privacy without sufficient justification.[3]

What we can take from these decisions is that arbitrary surveillance and/or recording of employees' activities ought to be avoided. If you have a legitimate business or security reason to implement a surveillance system in the workplace, consult whether or not it is the least intrusive method and ensure that employees are informed.

3. Breathalyzers on ignitions

An ignition interlock device is an in-car alcohol breath screening device that prevents a vehicle from starting if it detects a blood alcohol concentration over a pre-set limit. The device is typically located inside the vehicle, near the driver's seat, and is connected to the engine's ignition system. Before you start your vehicle, you need to blow into the device. If your blood alcohol concentration is over the pre-set limit, your vehicle will not start.

This would foreseeably be an issue for employees that are required to use an ignition interlock device following a drunk-driving offence. Could an employer choose to implement this device in its vehicles? If an employee had use of such a device as a bail condition, they could freely do so on their own vehicle. The employee would be required to inform the employer before such an installation; however, policies addressing such matters are presumably rare.

While the concept of ensuring employees are not driving vehicles with blood alcohol over legal limits sounds "admirable", it has not been subject to judicial consideration and, as it is collecting health information, should be approached with extreme caution. It falls under the legal landscape of "random drug/alcohol testing. The Supreme Court has held that employers must lead evidence of a general workplace drug or alcohol problem in order to justify random drug and alcohol testing policies.[4]

C. Devices for Entry

Biometric entry devices have the advantage of being personalized to each employee, making it easy to grant and remove access ensuring that secure entry is only provided to current

---

[3] *Colwell v. Cornerstone Properties Inc.*, [2008] O.J. No. 5092 (S.C.J.).
[4] *Communications, Energy and Paperworkers Union of Canada, Local 30 v. Irving Pulp & Paper, Ltd.*, 2013 SCC 34.

employees. Some systems double as a time tracking system for employee arrival, departure, and break times.

1. Fingerprinting and Retinal Scans ("Biometric Systems")

Employers in Canada are beginning to use biometric systems to replace traditional lock-and-key or card-swipe systems. These sensors record a person's fingerprint-like image to create a digital formula which a computer can use to unlock the device/door. Typically, the image is deleted from the system, and the formula is saved on the computer. Although using biometrics is not the same as storing an employee's fingerprint, employees and unions have complained against it. The general argument is that biometrics invades an employee's privacy rights and, in some cases, their rights under the *Charter of Rights and Freedoms*.[5]

In the unionized context, the starting point is with the widely accepted principle that rules unilaterally imposed by an employer must not be unreasonable or inconsistent with the collective agreement.[6] This principle has been applied in cases considering the employer's implementation of biometric systems.

For example, in *Metropolitan Toronto (Municipality) v. C.U.P.E., Local 79*,[7] the union filed a policy grievance alleging that the City of Toronto violated the collective agreement by implementing a policy of security checks for certain employees engaged in janitorial and maintenance work. The union alleged that a policy of security checks—which included fingerprinting as "keys" for locked doors after hours—was an unreasonable exercise of management rights and was contrary to their rights against unreasonable search and seizure under the *Charter*.

While the arbitrator determined that there was clear evidence for both the requirements and the mechanics of security checks, in this instance, the procedure for implementing these security checks was in violation of the collective agreement because it did not provide a system of review. That lack of review "in effect" deprived an aggrieved employee from exercising his or her rights; it was not open to the employer to impose such a regime unilaterally.[8] While this case was not necessarily decided on the merits, it does reinforce the idea that employers should inform employees before implementing biometric systems to prevent backlash.

In *Agropur (Natrel) v. Teamsters Local Union No. 647*,[9] a milk producer introduced biometrics in relation to time-keeping in order to eliminate the occurrence of some employees "punching in" on other employees' behalves, also known as "buddy-punching". The union argued that buddy-punching was not a serious problem at the plant, and that the employer could use a less intrusive method. While the employer acknowledged that the biometric system involved some

---

[5] *Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s. 8.
[6] *Re Lumber and Sawmill Workers' Union, Local 2537 and KVP Co. Ltd.*, [1965] O.L.A.A. No. 2.
[7] *Metropolitan Toronto (Municipality) v. C.U.P.E., Local 79*, [1998] O.L.A.A. No. 52.
[8] *Metropolitan Toronto (Municipality) v. C.U.P.E., Local 79*, [1998] O.L.A.A. No. 52, para 29.
[9] *Agropur (Natrel) v. Teamsters Local Union No. 647*, [2008] O.L.A.A. No. 694.

invasion of privacy, it maintained that the benefits outweighed any intrusion and that the collective agreement did not limit the rights of the employer to do so. The arbitrator ultimately held that the employer's implementation of a fingertip scan was reasonable; eliminating "buddy-punching" was enough of a legitimate business reason to outweigh any intrusion on employee privacy rights, which was, in any event, minimal.

Further, in *Gerdau Ameristeel v. U.S.W., Local 8918*, the employer steel mill sought to implement a biometric scan system to record its employees' work time and attendance. The union brought a grievance alleging that the employer made this decision unilaterally, contrary to the collective agreement. However, the arbitrator held that the employer did not contravene its substantive or procedural obligations under the collective agreement; biometric scanning in this case did not photograph the fingertip (only measurements of ridges and valleys were used to create an algorithm which is linked to a name or employee ID).[10] Given that the work environment at the plant was inherently dangerous (involving a smelting process), the employer's reasons for seeking introduction of the biometric scan system were legitimate.

Based on such decisions, employers should therefore be in a position to show the following:

a) The collective agreement/employment agreement does not prohibit biometric systems;
b) There is a legitimate business purpose for implementing a biometric systems;
c) There is a minimal infringement on privacy rights; and
d) The benefit outweighs any infringement on privacy rights.

2. Computer signing in and out

The Supreme Court has determined that employees have a diminished but reasonable expectation of privacy in their use of their workplace computers.[11] In light of this determination, it is recommended that employers ensure their employees are aware that they should have no expectation of privacy in that regard, and that their signing in and out of these computers is tracked.

3. Voice Recognition

Voice recognition technology is another potential method of granting security clearance and access in the workplace. To work, typically, the computer must store the voice print of the user so that the user can be recognized. While this technology is still expensive and not frequently utilized, there is one decision on point.

The Federal Court in *Turner v. Telus Communications Inc.*[12] considered the introduction of a new technology called "e.Speak", which used voice recognition technology to allow employees to use and access the company's internal computer network by speaking commands through

---

[10] *Gerdau Ameristeel v. U.S.W., Local 8918*, [2011] O.L.A.A. No. 405 (ON LA), at para 12.
[11] *R. v. Cole*, 2012 SCC 53.
[12] *Turner v. Telus Communications Inc.*, 2007 FCA 21.

the telephone. The company made it known that employees who failed to use this new software would face progressive discipline. Employees then filed an application with the Ontario Privacy Commissioner pursuant to the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*")[13] for a declaration that the company's collection of voice prints was an unlawful invasion of the employees' privacy.

The Privacy Commissioner decided in the employer's favour, and the decision was upheld by the Federal Court on judicial review. The Federal Court found that the company was under the obligation to obtain consent before collecting the voice characteristics of employees—since "e.Speak" only applied to those who consented to enrolment, the Federal Court found that it did not violate the provisions of *PIPEDA* and was a proper workplace system introduced by the employer.

As a general rule, if the system does not forego the collection of consent from employees, and if the procedure for implementing the device for entry has an avenue to hear employee concerns, adopting such technology in the workplace should be permissible.

The author expects that the analysis would be much the same in this area as it would in fingerprint/retinal scan technology if subjected to a similar challenge.

D. Payment

Electronic payment into an employee's bank account has also been subject to review. It requires disclosure of banking information and has been challenged and/or refused on the basis of infringement of privacy. Consent can be implied for certain categories of personal information in order to facilitate the administration of the employer-employee relationship. For example, an employer may have to disclose an employee's SIN, banking information (branch, account number, etc.), and address to a payroll administrator in order for the employee to get paid. Nowadays, electronic payment is widely accepted.

1. Bank Information for Electronic Payment

For federal government employees, the information they provide for the purposes of enrolling in direct deposit payroll is protected under the *Privacy Act*,[14] and access to their respective accounts is protected by agreements with their financial institution.

For the private sector, the *PIPEDA* applies to the management of personal information. While the *PIPEDA* definition of "personal information" can encompass banking information,[15] an individual's right to object to its disclosure for direct deposit/electronic payment has not yet been considered.

---

[13] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 14(1).
[14] *Privacy Act*, R.S.C., 1985, c. P-21.
[15] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1).

Further, the *Employment Standards Act, 2000* ("*ESA*")[16] is silent on the matter of payment by direct deposit. Provisions regarding payment of wages under the *ESA* only state that agreements can be made to pay an employee's wages by direct deposit into an institution that does not have an office or facility within a reasonable distance from where the employee usually works.[17]

However, a number of labour arbitration decisions demonstrate the now universal acceptance of direct deposit systems.[18] Even in past occasions where employees objected (wanting, for example, to be paid by cheque), it has been held that the legitimate business decisions of the employer outweigh the availability of personal payment options for employees.

From this we can likely conclude such practice is reasonable and employees may not be permitted to opt out from direct deposit.

E. Pre-hiring Screening Devices

The biggest problem with using the technology of pre-hiring screening is the "extra" information it provides or may provide irrelevant to the hiring process and which may be used to then discriminate under human rights legislation.

1. Credit Checks

A recent decision from Alberta is instructive for employers who perform credit checks as part of the hiring process. The Office of the Information and Privacy Commissioner of Alberta found that an employer who conducted pre-employment credit checks of applicants for the position of retail sales associate breached the requirements of the province's privacy legislation.[19]

The employer was concerned about the incidence of in-store theft and implemented pre-hire credit checks to assess how applicants would handle the financial responsibilities of being a sales associate, and assess whether applicants had a probable risk of in-store theft or fraud. The officer who investigated the matter found that the employer had not established that a credit report was reasonably required to assess a person's ability to perform the duties of a sales associate, or how this information links to a person's likelihood to commit theft or fraud.

For Ontario businesses, there is nothing to suggest an employer cannot perform a credit background check on anybody employed with their company or who has applied for

---

[16] *Employment Standards Act, 2000*, S.O. 2000, c. 41.
[17] *Employment Standards Act, 2000*, S.O. 2000, c. 41, s. 11(4)
[18] *Victoria Hospital Corp. v. London & District Service Workers' Union, Local 220*, 1982 CarswellOnt 2458 (ON LA); *Siemens Vdo Automotive Inc. v. CAW-Canada, Local 127*, 2004 CarswellOnt 5472 (ON LA).
[19] *Investigation Report P2010-IR-001*, Office of the Information and Privacy Commissioner of Alberta (2010) <https://www.oipc.ab.ca/news-and-events/news-releases/2010/investigation-report-p2010-ir-001.aspx>

employment with their company. The Ontario *Human Rights Code* (the "*Code*")[20] does not prohibit refusal to hire a prospective employee as a result of an undesirable result when checking their credit history. However, we may see that develop.

2. Criminal Background Checks

Where reasonable grounds exist to believe that an employee has been convicted of a criminal offence which could materially affect the performance of his/her duties, an employer may be justified in seeking consent to disclosure of police or criminal records. Some types of employment (e.g. airport security; supervision of vulnerable children) may, by their nature, warrant constant scrutiny; however, a general broad policy may be struck down as an invasion of privacy.

The Supreme Court of Canada has emphasized that the purpose of extending anti-discrimination law to those convicted of criminal offences is to protect them from the unjustified and indefinite social stigma that operates to exclude people with a criminal conviction from the labour market well after sentences are served and a pardon has been obtained.[21]

In order for an employer to seek a criminal background check, it must establish a compelling link between its policy requiring the disclosure of the criminal records and workplace safety or other legitimate business purpose. A policy for criminal checks must also be consistent with ss. 5(1) and 5(2) of the *Code* which prohibits discrimination and harassment in employment with respect to "record of offences."[22]

A prime example comes from the labour arbitration decision of *CAW-Canada, Local 2098 v. Diageo Canada Inc.*[23] The employer started to use pre-employment criminal background checks for new hires. From the union's perspective, this was an unjustified interference with the privacy rights of employees. The arbitrator permitted the employer's use of criminal background checks because the employer was able to demonstrate the following:

a) The policy specifically applied to sensitive roles, rather than to *all* positions at the plant.
b) The policy, on its face, set out three categories of employees who were to be exempted from background checks.
c) There was an appeal mechanism in the collective agreement should the result of a criminal background check disadvantage an employee.
d) The policy in question reflected a corporate-wide initiative; the future intent of the employer to extend the policy to other sites and plans was evidence that the employees at this plant had not been singled out for special treatment.

---

[20] *Human Rights Code*, R.S.O. 1990, c. H. 19.
[21] *Quebec (Commission des droits de la personne et des droits de la jeunesse) v. Maksteel Quebec Inc.*, 2003 SCC 68.
[22] *Human Rights Code*, R.S.O. 1990, c. H. 19, s. 5(1)-(2).
[23] *CAW-Canada, Local 2908 v. Diageo Canada Inc.*, [2010] O.L.A.A. No. 21.

Further, in *Dubé v. CTS Canadian Career College,*[24] the Ontario Human Rights Tribunal found that discrimination occurred when the company withdrew a job offer it had previously made to the applicant, after learning of his criminal history and failed to provide a lawful reason for the decision. The corporate employer was responsible for damages arising from its discriminatory hiring decision.

These decisions indicate that an employer cannot arbitrarily conduct criminal background checks without sufficient justification. If the employer has a legitimate business and/or security reason for criminal background checks in pre-hiring, it is recommended that the employer have a thorough policy in place that includes how the checks will be conducted and to whom they will apply.

3. Social Media Searches

Searching prospective employees' social media pages can be subject to some risks. While there are fewer restrictions upon an employer's ability to conduct social media background checks on employees or prospective employees, all individuals have some privacy rights. The Ontario Court of Appeal has held that an intentional or reckless "intrusion upon seclusion" of another's private affairs or concerns is subject to liability if the invasion would be highly offensive to a reasonable person.[25]

A simple Google or Facebook search on a job candidate that reveals information not restricted or password-protected likely would not satisfy the test for "intrusion upon seclusion". For example, a recent case from New Brunswick held that there is no expectation of privacy with respect to a public posting on Facebook; the court declined to find that the employer invaded the employee's private affairs by accessing her Facebook page.[26] However, employers that take more invasive or deceptive actions (i.e. by demanding candidates' social media passwords) could be at risk.

Job candidates' public online profiles are often reviewed by employers and recruiters as part of the hiring process, provided that hiring decisions are made on the basis of legitimate job qualifications that are thereby revealed and not on any human rights' grounds. They do, of course, potentially expose the employer to the suggestion of discrimination and are far from ideal for most positions.

---

[24] *Dubé v. CTS Canadian Career College*, 2010 HRTO 713.
[25] *Jones v. Tsige*, 2012 ONCA 32, para 19.
[26] *Rancourt-Cairns v. Saint Croix Printing and Publishing Company Ltd.*, 2018 NBQB 19.

F. Resulting Themes

What we have learned:

1. Do not collect information without advising the employee(s).
2. Make it clear if something is a condition of employment by including it in the job offer.
3. Implement policies for new advancements in technology as they are introduced to the workplace.
4. Utilize the least invasive method for the business need when there is any impact on personal time/space.
5. Avoid collection of or access to information which can even arguably be used to discriminate.

The Cheat Sheet

An overview of specific topics covered in more detail above:

GPS Tracking/ Recording	Implementing systems for surveillance of employees should be approached with caution; however, measures developed with the purpose of enhancing the protection of employees (and of which employees have subsequently been informed) can be permitted. For example, an employer is allowed to monitor a vehicle's use through GPS and other navigation systems as a legitimate way to protect the employer's asset.
Biometric Systems	Biometric systems, including finger print and retinal scan technology, are often implemented by the employer for security purposes, or to replace traditional attendance monitoring (i.e. card-swiping or punching in and out). Employers should be in a position to show the following: • The collective agreement/employment contract does not prevent biometric systems • There is a legitimate business purpose • There is a minimal infringement on privacy rights • The benefit outweighs any infringement on privacy rights
Banking information	For federal government employees, the information they provide for enrolment in direct deposit is protected under the *Privacy Act*, and access to their respective accounts is protected by agreements with their financial institution. While banking information can be captured in the definition of "personal information" under *PIPEDA*, this issue has not yet been judicially considered. Furthermore, there is nothing in the *ESA* to suggest that an employee has a right to oppose payment of wages by direct deposit. Direct deposit/electronic payment is now, essentially, a universally accepted method of payment of wages. Even in past occasions where employees objected (wanting, for example, to be paid by cheque) it has been held that the legitimate business decisions of the employer outweigh the availability of personal payment options for employees.
Pre-Hiring: Criminal Background Checks and Social Media Searches	An employer must establish a compelling link between its policy requiring disclosure of the criminal records and workplace safety or other legitimate business purpose. Policy for criminal checks must also be consistent with the Ontario *Human Rights Code* which prohibits discrimination and harassment in employment with respect to "record of offences." Job candidates' public online profiles are often reviewed by employers and recruiters as part of the hiring process, provided that hiring decisions are made on the basis of legitimate job qualifications that are thereby revealed and not on any human rights grounds.